Notes for Algebraic Structures

Spring 2016

Transcribed by Jacob Van Buren
(`jvanbure@andrew.cmu.edu`)

Notes for Algebraic Structures, taught Spring 2016 at Carnegie Mellon University, by Professor Clinton Conley.

Administrativia

Instructor. Clinton Conley (`clintonc@andrew.cmu.edu`), WEH 7121
`http://www.math.cmu.edu/~clintonc/`

Grading. 20% HW, 20% $\times$ 2 midterms, 40% Final

Homework. Wednesday-Wednesday. Graded for completeness, one starred problem for which no collaboration of any type is allowed.
Most homework out of textbook ("D&F").

Contents

The Integers

Lecture 1 (2016–01–11)

NOTATION. $\mathbb{N} := \{1, 2, 3, \ldots\}$ in this class.

Properties: Order, other things. Least element in a set S: $x \in S$ s.t. $\forall y \in S, x \leq y$
Addition $(\mathbb{Z}, +)$:

- Associativity $(x + y) + z = x + (y + z)$
- Identity $x + 0 = 0 + x = 0$
- Inversion $x + (-x) = (-x) + x = 0$
- Commutativity $x + y = y + x$

Multiplication $(\mathbb{Z}, +, \cdot)$:

- Associative
- Distributive
- Identity ("1")

Integer division: Assume x an integer and $y \in \mathbb{Z}^+$ then $\exists! d \in \mathbb{Z}, \exists! r \in \mathbb{Z} : 0 \leq r < y, x = d \cdot y + r$

DEFINITION 1. $y|x$ "y divides x" iff $\exists d \in \mathbb{Z} : x = d \cdot y$.

E.g. $3|9, 4 \not| 7$.

DEFINITION 2. d is a gcd of x and y if

- $d|x, d|y$
- If $c|x$ and $c|y$ then $c|d$

Lecture 2 (2016–01–13)

DEFINITION 3. Given $a, b \in \mathbb{Z}$, denote by $\mathbb{Z}(a, b)$ the set $\{ax + by | x, y \in \mathbb{Z}\}$.

THEOREM 4 (Euclid, Bezout). *Suppose $a, b \in \mathbb{Z}$ are nonzero and let d be the smallest positive element of $\mathbb{Z}(a, b)$, then d is the unique positive GCD of a and b.*

PROOF. d is a gcd of a, b

(1) (Existance of positive GCD)
  (a) By integer division, $\exists q \in \mathbb{Z}, \exists r \in \mathbb{Z}$ with $0 \leq r < d$ such that $a = qd + r$. If $r = 0$ then $d|a$, so done. Otherwise, suppose $0 < r < d$, so $r = a - qd$ since $d \in \mathbb{Z}(a, b)$, we may fix x, y st $d = ax + by$, meaning $r = a - q(ax + by) = a(1 - qx) + b(-qy)$, so $r \in \mathbb{Z}(a, b)$, meaning d was not the minimal positive element in $\mathbb{Z}(a, b)$, RAA. Thus, $d|a$
  (b) HW: If $c|a$ and $c|b$ then $c|(ax + by)$ for all $x, y \in \mathbb{Z}$ Hence $c|d$

(2) (Uniqueness of positive GCD) Suppose d_1, d_2 are both positive gcds of a and b. $d_1|d_2$ and $d_2|d_1$ as they are both gcds. i.e., $\exists m, n \in \mathbb{Z}$ such that $d_2 = md_1$ and $d_1 = nd_2$. As $\text{sgn}(d_1) = \text{sgn}(d_2)$, $m \geq 0$ and $n \geq 0$. As $d_1 = mnd_1$, $m = n = 1$. Thus $d_1 = d_2$.

□

Definition 5. Relatively prime $\iff$ $\gcd(a, b) = 1$

Theorem 6. *Suppose p is prime and $a, b \in \mathbb{Z}$ are nonzero, and $p|(ab)$ then $p|a$ or $p|b$.*

Proof. Consider $d = \gcd(p, a)$. Since $d|p$, we know $d = p$ or $d = 1$.
If $d = p$: By def of GCD, $d|p$ and $d|a$ ie. $p|p$ and $p|a$ so we're done.
If $d = 1$: Fix integers x and y such that $px + ay = 1$. $b = p(xb) + (ab)y$ as $p|p(xb)$ and $p|\underbrace{(ab)}_{\uparrow}y$, $p|b$.

□

Theorem 7 (Unique Prime Factorization). *Suppose that $a > 1$ an integer, $m, n \geq 1$ and $p_1 \leq p_2 \leq \ldots \leq p_m, q_1 \leq q_2 \leq \ldots \leq q_m$ are positive primes.*

Then $m = n$ and $p_i = q_i$ for all i.

Proof. By induction, it suffices to show $p_1 = q_1$. Suppose not. WLOG, assume $p_1 < q_1$. We know that $p_1|a$ (as $p_1|q_1q_2 \ldots q_n$) Hence, $\exists i \leq n$ such that $p_i|q_i$. since p_i and q_i prime, $p_1 = q_i$. However, $p_1 < q_1 \leq q_i = p_1$ so $p_1 < p_2$ contradiction.
Hence $p_1 = q_1$ so by induction, we're done. □

Lecture 3 (2016–01–15)

Teaser: Construct numbers of the form $a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.
Notion of addition still exists: (similar to complex numbers, coefficients remain integers)
Same with multiplication
Among these "numbers", 2 is irreducible. But, 2 is not prime, as $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 + \sqrt{-5})$, but $2|\underbrace{(1 + \sqrt{-5})(1 - \sqrt{-5})}_{=6=2\cdot 3}$.

The Integers (mod n)

For today, $n > 0$.

DEFINITION 8. For $a, b \in \mathbb{Z}$ we say $a \equiv b \pmod{n}$ iff $n \,|\, (b-a)$.

$\equiv$ is an *equivalence relation*

- Reflexivity: $a \equiv a$
- Symmetry: $a \equiv b \iff b \equiv a$
- Transitivity: $a \equiv b \wedge b \equiv c \implies a \equiv c$

PROOF. We know that $a \equiv b$ and $b \equiv c$, i.e. $n \,|\, (b-a)$ and $n \,|\, (c-b)$ We want $a \equiv c$, i.e., $n \,|\, (c-a)$

$$c - a = c + (-b + b) - a = \underbrace{(c-b) + (b-a)}_{n \text{ divides these}}$$

$\square$

DEFINITION 9. Denote by $\overline{a}$ or $[a]_n$ the <u>equivalence class</u> of a with respect to $\equiv \pmod{n}$ (I.e., The set $\{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = \overline{\{a + kn : k \in \mathbb{Z}\}}$).

EXAMPLE. If $n = 2$, there are 2 equivalence classes:
$\overline{0} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \overline{2} = \overline{-36}$
$\overline{1} = \{\ldots, -3, -1, 1, 3, \ldots\}$

DEFINITION 10. Denote by $\mathbb{Z}/n\mathbb{Z}$ the collection of all $\equiv \pmod{n}$ equivalence classes.

E.g. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$
"Define" addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ as follows:

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Makes sense, but we need to check that this definition makes any sense at all (make sure it's *well-defined*). Specifically, we need to make sure that the results of these operations doesn't depend on the representatives of the equivalence classes we chose (e.g. check that $\overline{x} + \overline{z} \equiv \overline{y} + \overline{z}$ if $x \equiv y$).
For brevity, we just show addition.

THEOREM 11. $+$ *and* $\cdot$ *are well-defined on* $\mathbb{Z}/n\mathbb{Z}$

PROOF. (of $\cdot$) Assume that $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then, we want to show that $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.
We know: $n \,|\, (a_2 - a_1)$ and $n \,|\, (b_2 - b_1)$.

We want: $n \,|\, (a_2b_2 - a_1b_1)$.

$$\begin{aligned} a_2b_2 - a_1b_1 &= a_2b_2 + (-a_1b_2 + a_1b_2) - a_1b_1 \\ &= (a_2b_2 - a_1b_2) + (a_1b_2 - a_1b_1) \\ &= \underbrace{(a_2 - a_1)b_2 + a_1(b_2 - b_1)}_{n \text{ divides these}} \end{aligned}$$

So, $n \,|\, (a_2b_2 - a_1b_1)$ as desired □

Remark: This is a special case of a "quotient construction," in which you start with a set and an equivalence relation on it and operations on the set that "respect" the equivalence relations (i.e. equivalent inputs yield equivalent outputs)
Moar notes: Mutiplicative inverses are uncommon in the integers (only for 1 and -1). However, it's "more prevalent" in $\mathbb{Z}/n\mathbb{Z}$ in the following sense:

THEOREM 12. *Suppose $n > 0$ is an integer, $a \in \mathbb{Z}$ such that $\gcd(n, a) = 1$ (they're coprime). Then there is $b \in \mathbb{Z}$ such that $ab = 1 \pmod{n}$ (alternatively, $\overline{a} \cdot \overline{b} = \overline{1}$)*

PROOF. Use Bezout's theorem (from last lecture) Take integers x, y such that $nx + ay = \gcd(a, n) = 1$. Then, $nx = 1 - ay$, so $n \,|\, (1 - ay)$, so $1 \equiv ay \pmod{n}$, Choose $b = y$ and we're done ($\overline{a}\overline{b} \equiv \overline{1}$). □

Groups

Definition 13. We say that $*$ is a binary operation on some set X if it is a function $* : X \times X \to X$. (That is, $*$ accepts two (ordered) inputs from X and it outputs one element of X.)

Remark: usually write $a * b$ for the output of $*$ on the input (a, b).

Definition 14. A group is a set G with a binary operation $*$ (often abbreviated $(G, *)$) satisfying the following 3 axioms.

i. Associativity: $\forall a, b, c \in G : (a * b) * c = a * (b * c)$
ii. Identity: There is some $e \in G$ such that $\forall a \in G : a * e = e * a = a$
iii. Inversion: $\forall a \in G(\exists b \in G(a * b = b * a = e))$ (where e is as described in ii)

Lecture 4 (2016–01–20)

Recall the definition of a group.

Definition 15. $(G, *)$ is an abelian (commutative) group if it is a group and

iv. $(G, *)$ is commutative $(\forall x, y \in G : x * y = y * x)$

Let $(G, *)$ be an arbitrary but fixed group.

Proposition 16. *There is a unique identity element.*

Proof. Suppose e and f both satisfy the second group property. we compute $e * f$ in two ways. $e * f = f$ and $e * f = e$, so by transitivity, $e = f$. $\square$

Proposition 17. *If $a \in G$, a has a unique inverse.*

Proof. Suppose that b and c are both inverses for a, $b * a = e$, $a * c = e$. Then,

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c$$

$\square$

Notational Conventions.

- We will often just call a group G instead of $(G, *)$
- We abbreviate multiplication $(x * y)$ as $x \cdot y$ or just xy
- We will often write xyz for $(x * y) * z$ (due to associativity)
- When working with $(\mathbb{Z}, +)$, we'll just use $+$
- We'll denote the (unique) identity of G by 1 or by e.
- We'll denote the inverse of x by x^{-1}
- Given an integer exponent $n \in \mathbb{Z}$ and $x \in G$, define

$$x^n = \begin{cases} \prod_{i=1}^{n} x, & \text{if } n > 0 \\ e, & \text{if } n = 0 \\ \prod_{i=1}^{-n} (x^{-1}), & \text{if } n < 0 \end{cases}$$

Group Examples. "Definition:" $\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}^+ \right\}$

(1) $(\mathbb{Z}, +)$ is an abelian group
(2) $(\mathbb{Z}, \times)$ is not a group
 Why? 2 has no inverse in $\mathbb{Z}$. $(\nexists x \in \mathbb{Z} : (2x = 1))$
(3) $(\mathbb{Q}, +)$ is an abelian group
(4) $(\mathbb{Q}, \times)$ is not a group (0 has no inverse)
(5) $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group.
(6) $\mathrm{GL}(n)$ is the set of matricies $A_{n\times n}$ for which $\det A_{n\times n} \neq 0$
(7) The set G of 2×2 matrices with determinant 1, along with matrix multiplication, is a group. Called the "special linear group."

Closure:

$$\det\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \cdot \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix} \right) \right) = (bc - ad)(fg - eh) = 1$$

 i. Associativity: proof left for the reader.
 ii. Identity: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$
 iii. Given $a = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$, take $a^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix} \right)$, which you can verify is still in G.

 The group is *not* abelian. Take $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right), b = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix} \right)$. Verify that $ab \neq ba$

(8) Suppose that $X \neq \emptyset$ is some set, and denote by S_X the set of bijections $f : X \to X$. Then $(S_X, \circ)$ is a group, where $\circ$ is function composition. ($(f \circ g)$ is the function $x \mapsto f(g(x))$.)
 Identity is $x \mapsto x$. Inversion $f^{-1} = f^{-1}$.

Symmetric Groups

Lecture 5 (2016–01–25)

Recall: if X is a set then S_X is the group of bijections on it.

Definition 18. S_X (or Sym_X) is called the symmetric group on X.

Note: $\circ$ is associative because $(f \circ g) \circ h$ is

$$x \overset{h}{\mapsto} (x) \overset{g}{\mapsto} g(h(x)) \overset{f}{\mapsto} f(g(h(x)))$$

Note: if $X = \{1, \dots, n\}$, then we usually write $\underline{S_n}$ instead of $S_{\{1,\dots,n\}}$. (Sometimes called symmetric group of degree n.)
Let's examine S_3:

elt.	1	2	3
e	1	2	3
a	1	2	3
b	1	3	2
c	2	3	1
d	3	1	2
f	3	2	1

The group has $6 = 3!$ elements.
Lets compute ab and ba
$ab = a \circ b$, looking it up in the table gives $ab = d$ and $ba = c$.
In particular, S_3 is not abelian.

Definition 19. A cycle is a permutation σ of the following form:

There is a sequence $x_1, x_2, \dots, x_m$ of finitely many (distinct) elements of $\{1, 2, \dots, n\}$ such that $\sigma(x_{i-1}) = x_i$, $\sigma(x_m) = x_1$, and $\sigma(y) = y$, for $y \notin \{x_1, \dots, x_m\}$.
We call m the length of the cycle.

Ex. In S_3, $d = \frac{1\,2\,3}{3\,1\,2}$ is a cycle of length 3, with $x_1 = 1, x_2 = 3, x_3 = 2$.

Ex. In S_3, $a = \frac{1\,2\,3}{1\,3\,2}$ is a cycle of length 2, with $x_1 = 2, x_2 = 3$.

Notation. Given a cycle, we can efficiently denote it by $(x_1\, x_2\, x_3\, \dots\, x_m)$.

Example. In S_3, $a = \frac{1\,2\,3}{1\,3\,2}$ would be written as (1 3 2).

Let's work in S_5.
$\varphi := \frac{1\,2\,3\,4\,5}{3\,4\,1\,5\,2}$ is not a cycle, but it is the "superposition" of two cycles (1 3) and (2 4 5). Thus, we may write $\varphi =$(1 3) $\circ$ (2 4 5), or (2 4 5)(1 3).

Theorem 20. *Every permuation in S_n may be written as the product of "disjoint" cycles. (The identity is the empty product).*

PROOF. Sketch: If youa have e then you're done trivially.
Otherwise, fix the least element x of $\{1, \ldots, n\}$ "moved" by σ (i.e. $\sigma(x) \neq x$). Look at $x, \sigma(x), \sigma^2(x), \ldots, \sigma^m(x) = \sigma^n(x)$, $n < m$. So, as σ is invertible, $\sigma^{m-n}(x) = x$, so x is part of a cycle. $\square$

THEOREM 21. *Cycles can be written as a product of transpositions.*

General propositions on inversion in groups. Let G be a group, and let $a, b, x \in G$ be arbitrary.

- $(a^{-1})^{-1} = a$

  PROOF. Show that a is the inverse of a^{-1}. Follows from group axiom. $\square$

- $(ab)^1 = b^{-1}a^{-1}$

  PROOF. $(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$. Similarly, this works when we multiply from the other side. $\square$

Lecture 6 (2016–01–27)

DEFINITION 22. The <u>cardinality</u> (or <u>order</u>) of a group G is the number of elements in it, denoted by $|G|$.

EXAMPLE.

- $|\mathbb{Z}| = \infty (= \aleph_0)$
- $|(\mathbb{Z}/5\mathbb{Z})| = 5$
- $|S_4| = 4! = 24$

DEFINITION 23. Given a group G and $x \in G$, the <u>order</u> of x is the smallest integer $n > 0$ such that $x^n = e$. If no such n exists, we say the order is ∞.
We denote by $|x|$ the order of x.

EXAMPLE. In $(\mathbb{Z}, +)$: $|0| = 1$, $|5| = \infty$.
In S_5: $|(1\ 3)| = 2$, $|(2\ 4\ 5)| = 3$, $|(1\ 3)(2\ 4\ 5)| = 6$.

PROPOSITION 24. *If G is a* finite *group, every $x \in G$ has finite order. Moreover, $|x| \leq |G|$.*

PROOF. Say $|G| = k$. Consider the sequence $x^0, x^1, x^2, \ldots, x^k$. There are $k + 1$ items in the sequence. So $\exists m < n$ such that $x^m = x^n$. $x^{n-m} = x^n x^{-m} = x^m x^{-m} = e$. As $0 < n - m \leq k$, it follows that $|x| \leq n - m \leq |G|$. $\square$

Subgroups

Definition 25. Suppose $(G, *)$ is a group and $H \subseteq G$ some subset of G. We say H is a <u>subgroup</u> of G, written $H \leq G$ if $(H, *)$ happens to be a group, i.e., the following properties hold:

$*$ is a associative binary operator on H (i.e., it's closed) with inverses and an identity element.

Example.

- $\mathbb{Z} \leq \mathbb{Q}$ (under addition)
- Even integers $\leq \mathbb{Z}$ (under addition)
- $n\mathbb{Z} \leq \mathbb{Z}$, where $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$
  Aside: every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$
- $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq S_4$.

Proposition 26. *(HW): $H \leq G$ iff*
(a) $H \neq \emptyset$ (nonempty)
(b) $\forall x, y \in H (xy \in H)$ (closed under product)
(c) $\forall x \in H (x^{-1} \in H)$ (closed under inverses)

Proposition 27. *Suppose G is a* finite *group. Then $H \leq G$ iff $H \neq \emptyset$ and $\forall x, y \in H$: $xy \in H$.*

Proof. We show that for $H \subseteq G$ (a) and (b) $\implies$ (c) (letters from proposition (26)) Fix $x \in H$. Since G is finite, $|x|$ is finite (in G). Say $|x| = n > 0$ $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} = e_G$.

Hence, $e_G \in H$.
Examine x^{n-1}.

$$x^{n-1} = \begin{cases} x^0 = e & \text{if } n = 1 \\ \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} & \text{if } n > 1 \end{cases}$$

But $x^{n-1} = x^{-1}$, since $x^{n-1}x = x^n = xx^{n-1} = e$. Thus, (c) holds for H. $\square$

Remark. $\mathbb{N} = \{0, 1, \ldots\} \subseteq \mathbb{Z}$, but $\mathbb{N} \not\leq \mathbb{Z}$, despite satisfying (a) and (b).

(Left) Coset equivalence

Suppose G is a group and $H \leq G$ is a subgroup of G.

DEFINITION 28. We say $x \sim y \pmod{H}$ if $x^{-1}y \in H$.

PROPOSITION 29. $\sim \pmod{H}$ *is an equivalence relation.*

PROOF.

- Reflexivity ($x \sim x$):
  $x^{-1}x = e \in H$, so $x \sim x$.
- Symmetry ($x \sim y \implies y \sim x$):
  We know $x^{-1}y \in H$. H is closed under inversion, so $H \ni (x^{-1}y)^{-1} = (y^{-1}(x^{-1})^{-1}) = (y^{-1}x)$. Thus, $y \sim x$.
- Transitivity ($(x \sim y) \wedge (y \sim z) \implies (x \sim z)$):
  We know $x^{-1}y \in H$ and $y^{-1}z \in H$.
  Thus, $H \ni (x^{-1}y)(y^{-1}z) = x^{-1}ez = x^{-1}z$, so $x \sim z$.

$\square$

Index